Приложение
к приказу ФСБ России
от
№

Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

I. Общие положения

1. Настоящие Требования определяют требования к устанавливаемым и используемым на всей территории Российской Федерации техническим, программным, программно-аппаратным и иным средствам для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (далее – КИИ), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографическим средствам защиты такой информации (далее – средства, если не оговорено иное).

II. Общие требования к средствам, предназначенным для обеспечения безопасности значимых объектов КИИ

2. Средства, предназначенные для обеспечения безопасности значимых объектов КИИ, должны соответствовать требованиям:

2.1. Обеспечение выполнения следующих задач:

обнаружение компьютерных атак;

предупреждение компьютерных атак;

ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

поиск признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ;

криптографическая защита обмена информацией необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

Данные задачи могут реализовываться одним или несколькими программно-аппаратными или программными средствами.

2.2. Отсутствие принудительного обновления программного обеспечения (далее – ПО) и управления с территории иностранного государства.

2.3. Отсутствие возможности несанкционированной передачи информации, включая технологическую, в том числе их разработчику (производителю).

2.4. Возможность осуществления их модернизации силами российских организаций без участия иностранных организаций и организаций с иностранными инвестициями.

2.5. Обеспечение гарантийной и технической поддержкой российскими организациями без участия иностранных организаций и организаций с иностранными инвестициями.

2.6. Отсутствие недекларированных возможностей в ПО.

2.7. Наличие: резервных копий ПО, формуляр, руководство администратора. В формуляре средств в отдельном разделе должны быть приведены условия эксплуатации, средства и способы подключения к сетям электросвязи, в том числе к сети «Интернет».

3. В технических, программных, программно-аппаратных и иных средствах, предназначенных для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ), предупреждения, ликвидации последствий компьютерных атак должны быть реализованы функции:

собственной безопасности;

визуализации информации;

построения сводных отчетов;

хранения информации.

III. Требования к средствам в части обнаружения компьютерных атак

4. Средства в части обнаружения компьютерных атак должны обладать следующими функциональными возможностями:

сбор и первичная обработка информации, поступающей от источников событий информационной безопасности (далее – события ИБ)[1];

автоматический анализ событий ИБ и выявление компьютерных инцидентов (компьютерных атак);

ретроспективный анализ данных и выявление не обнаруженных ранее компьютерных инцидентов.

5. При осуществлении сбора и первичной обработки событий ИБ средства должны обеспечивать:

удаленный и локальный сбор событий ИБ;

сбор событий ИБ в непрерывном режиме функционирования, в случае потери связи – сразу после ее восстановления, а также по расписанию;

обработку поступающих событий ИБ и сохранение результатов их обработки;

сохранение информации о событиях ИБ, в том числе в исходном виде;

синхронизацию системного времени и корректировку временных значений в принимаемых событиях ИБ (корректировку настроек часовых поясов);

[1] Источниками событий ИБ могут являться: операционные системы, средства обнаружения вторжений (атак), межсетевые экраны, средства предотвращения утечек данных, антивирусное программное обеспечение, телекоммуникационное оборудование, прикладные сервисы, средства контроля (анализа) защищенности, средства управления телекоммуникационным оборудованием и сетями связи, системы мониторинга состояния телекоммуникационного оборудования, системы мониторинга качества обслуживания.

сбор информации непосредственно от источников событий ИБ, из файлов либо посредством агентов, размещенных на отдельных источниках событий ИБ;

встроенную поддержку различных источников событий ИБ и возможность разработки дополнительных модулей, обеспечивающих получение информации от новых источников событий ИБ.

6. При осуществлении автоматического анализа событий ИБ и выявления компьютерных инцидентов (компьютерных атак) средства должны обеспечивать:

отбор и фильтрацию событий ИБ;

корреляцию и агрегацию событий ИБ;

выявление компьютерных инцидентов, регистрацию способов их обнаружения;

возможность корреляции для распределенных по времени и (или) месту возникновения событий ИБ;

возможность корреляции для последовательности событий ИБ;

возможность просмотра и редактирования правил корреляции, а также обновления и загрузки новых правил;

автоматическое назначение приоритетов событиям ИБ на основании заданной критичности.

7. При осуществлении ретроспективного анализа данных и выявления не обнаруженных ранее компьютерных инцидентов средства должны обеспечивать:

выявление связей и зависимостей между полученными ранее данными (событиями ИБ, компьютерными инцидентами, информацией об уязвимостях и недостатках в настройке, справочной информацией и другими данными) и анализируемыми в данный момент времени событиями ИБ;

возможность настройки параметров проводимого анализа;

проведение поиска не обнаруженных ранее компьютерных инцидентов с использованием новых правил обнаружения.

IV. Требования к средствам в части предупреждения компьютерных атак

8. Средства в части предупреждения компьютерных атак должны обладать следующими функциональными возможностями:

сбор и обработка сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации[1];

сбор и обработка сведений об уязвимостях и недостатках в настройке ПО, используемого на объектах контролируемых информационных ресурсов;

учет угроз безопасности информации.

9. При осуществлении сбора и обработки сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации средства должны обеспечивать:

9.1. Сбор и обработку конфигурационной информации:

об объектах, функционирующих в составе контролируемых информационных ресурсов;

о сетевых моделях контролируемых информационных ресурсов;

о контролируемых информационных ресурсах;

об источниках событий ИБ, используемых в составе контролируемых информационных ресурсов;

о телекоммуникационном оборудовании, используемом в контролируемых информационных ресурсах.

9.2. Сбор и обработку справочной информации:

о репутации IP-адресов, доменных имен, DNS-серверов и почтовых серверов;

о владельцах IP-адресов, доменных имен, DNS-серверов и почтовых серверов;

о местоположении и географической принадлежности IP-адресов;

об известных уязвимостях;

о правилах обнаружения компьютерных атак (сведения о сигнатурах);

о бот-сетях, включая сведения об их управляющих серверах.

---

[1] В качестве справочной информации используется любая дополнительная информация, позволяющая идентифицировать контролируемые объекты.

9.3. Возможность расширения перечня используемой информации об инфраструктуре контролируемых информационных ресурсов и справочной информации.

9.4. Возможность добавления, просмотра и изменения сведений об инфраструктуре и справочной информации.

10. При осуществлении сбора и обработки сведений об уязвимостях и недостатках в настройке ПО, используемого на объектах контролируемых информационных ресурсов средства должны обеспечивать:

сбор и обработку данных о дате и времени проведения исследования контролируемых информационных ресурсов;

сбор и обработку сведений об исследуемых объектах контролируемого информационного ресурса (сетевые адреса и имена объектов, наименования и версии операционных систем, под управлением которых функционируют объекты);

формирование перечня выполняющихся сетевых служб (для каждого объекта контролируемого информационного ресурса);

формирование перечня выявленных уязвимостей и недостатков в настройке ПО (для каждого объекта контролируемого информационного ресурса);

возможность формирования обобщенных сведений, представляемых в Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ).

11. При осуществлении учета угроз безопасности информации средства должны обеспечивать:

создание и изменение формализованной записи об угрозе безопасности информации в ручном режиме;

создание формализованной записи об угрозе безопасности информации в автоматизированном режиме посредством взаимодействия с другими автоматизированными системами;

создание формализованной записи об угрозе безопасности информации в автоматизированном режиме посредством взаимодействия с НКЦКИ;

автоматизированный обмен информацией об угрозах безопасности информации с НКЦКИ;

создание и изменение инструкций по обработке угроз безопасности информации;

построение рабочих процессов обработки сообщений об угрозах безопасности информации и запросов от НКЦКИ.

V. Требования к средствам в части ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

12. Средства в части ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты должны обладать следующими функциональными возможностями:

учет и обработка компьютерных инцидентов;

управление процессами реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак;

обеспечение взаимодействия с НКЦКИ;

информационно-аналитическое сопровождение.

13. При осуществлении учета и обработки компьютерных инцидентов средства должны обеспечивать:

создание и изменение типов карточек компьютерных инцидентов, определение состава полей этих карточек и требований к заполнению полей;

определение статусной модели компьютерных инцидентов в зависимости от типа инцидента;

назначение категорий и приоритетов компьютерных инцидентов по заданным критериям;

создание и изменение соглашений об уровне услуг по обработке компьютерных инцидентов;

создание и изменение правил по обработке компьютерных инцидентов;

управление доступом к данным о компьютерном инциденте;

создание формализованной карточки компьютерного инцидента в ручном режиме;

создание формализованной карточки компьютерного инцидента в автоматизированном режиме посредством взаимодействия с другими автоматизированными системами и НКЦКИ;

создание формализованной карточки компьютерного инцидента из поступившего формализованного сообщения об угрозе безопасности информации;

учет формализованных карточек компьютерных инцидентов;

фильтрацию, сортировку и поиск хранимых карточек компьютерных инцидентов и сведений об инцидентах;

агрегирование записей о компьютерных инцидентах по заданным критериям;

регистрацию действий администраторов как по настройке средств, так и по процессу работы со сведениями о компьютерных инцидентах;

отслеживание времени внесения и сроков хранения данных, а также источников этих данных;

создание и изменение правил по обработке компьютерных инцидентов и ликвидации последствий компьютерных атак.

14. При осуществлении управления процессами реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак средства должны обеспечивать:

обогащение данных компьютерного инцидента данными из внешних систем и предоставление контекста компьютерного инцидента, включая сведения о программных и конфигурационных уязвимостях, которые содержатся в реквизитах компьютерного инцидента;

применение типовых сценариев реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак, а также задание правил их применимости на основании сведений об инциденте;

создание задач для внешних систем и сервисов с возможностью экспорта, импорта и отслеживания статуса этих задач посредством интерфейса прикладного программирования;

уведомление о регистрации новых компьютерных инцидентов, завершении длительных задач, а также об изменении их состояния;

поддержку принятия управленческого решения при реагировании на угрозу безопасности информации или компьютерный инцидент;

поддержку координации действий сил и использования средств реагирования на компьютерный инцидент;

контроль соглашений об уровне услуг по обработке компьютерных инцидентов и контроль устранения компьютерных инцидентов.

15. При осуществлении взаимодействия с НКЦКИ средства должны обеспечивать:

автоматизированный обмен сведениями согласно перечню информации о компьютерных инцидентах, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

учет формализованных карточек компьютерных инцидентов в соответствии с системой идентификации НКЦКИ;

оперативную коммуникацию со специалистами НКЦКИ.

16. При осуществлении информационно-аналитического сопровождения средства должны обеспечивать:

интерактивное формирование выборок данных, основанных на комбинациях атрибутов и объектов из карточек компьютерных инцидентов, сообщений об угрозах безопасности информации и выходящих за рамки стандартных отчетов;

реализацию расчетов прогнозных значений анализируемых показателей на основе ретроспективных данных из карточек компьютерных инцидентов и сообщений об угрозах безопасности информации.

VI. Требования к средствам поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ

17. Средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ должны обеспечивать:

контроль изменений параметров настроек телекоммуникационного оборудования сети электросвязи;

контроль изменений параметров настроек систем управления телекоммуникационным оборудованием и сетями электросвязи;

обнаружение в сети электросвязи признаков управления телекоммуникационным оборудованием;

обнаружение признаков компьютерных атак в сети электросвязи по значениям служебных полей (заголовков) протоколов сетевого взаимодействия, а также сбора, накопления и статистической обработки результатов такого обнаружения;

хранение копий трафика внутреннего сетевого взаимодействия сетей электросвязи субъектов КИИ, использующих при внутреннем и внешнем сетевом взаимодействии нестандартизированные протоколы или протоколы промышленного назначения;

анализ и выгрузку фрагментов копий трафика внутреннего сетевого взаимодействия субъектов КИИ, использующих при внутреннем и внешнем сетевом взаимодействии нестандартизированные протоколы или протоколы с закрытыми спецификациями;

возможность определять векторы распределенных во времени компьютерных атак и соотносить их с элементами как сетевой инфраструктуры, так и технологического процесса объекта КИИ;

возможность извлечения передаваемых файлов заданного типа из сетевого трафика;

сигнализацию и уведомление о фактах обнаружения признаков компьютерных атак;

сигнализацию и уведомление о нарушениях штатного режима функционирования средств;

наличие интерфейса (интерфейсов) передачи данных о сетевом трафике, в котором обнаружены признаки компьютерных атак, а также результатов сбора, накопления и статистической обработки такой информации.

VII. Требования к средствам криптографической защиты обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак

18. Средства криптографической защиты обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, должны быть сертифицированы в системе сертификации средств защиты информации.

VIII. Требования к средствам в части реализации функций собственной безопасности

19. Технические, программные, программно-аппаратные и иные средства, предназначенные для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ), предупреждения, ликвидации последствий компьютерных атак, в части реализации функций собственной безопасности должны обеспечивать:

идентификацию и аутентификацию администраторов;

разграничение прав доступа к информации и уровней доступа к функциям;

регистрацию событий ИБ;

обновление программных компонентов и служебных баз данных;

самотестирование и контроль целостности ПО;

резервирование и восстановление средств.

19.1. При осуществлении идентификации и аутентификации администраторов средства должны обеспечивать:

однозначную идентификацию администраторов;

аутентификацию администраторов с использованием паролей (в том числе временного действия) и (или) аппаратных средств аутентификации;

хранение паролей в закрытом виде;

автоматическое информирование о необходимости смены паролей.

19.2. При осуществлении разграничения прав доступа к информации и уровней доступа к функциям средства должны обеспечивать:

разграничение доступа на основе политик безопасности;

возможность блокирования и повторной активации учетных записей;

поддержку функций создания, редактирования и удаления пользовательских ролей и возможности настройки прав доступа для каждой роли;

блокирование доступа при превышении значения максимального периода отсутствия активности;

сигнализацию о несанкционированных попытках доступа к управлению средствами;

журналирование всех действий администраторов с момента авторизации.

19.3. При осуществлении регистрации событий ИБ средства должны обеспечивать:

возможность определения перечня событий ИБ, подлежащих регистрации, и сроков хранения соответствующих записей в журналах регистрации;

возможность регистрации как минимум следующих связанных с функционированием средств сведений: идентификатора администратора, времени входа и выхода, запуска (завершения) программ и процессов, связанных с реализацией функций безопасности средств, интерфейса (порта)

подключения, команды управления, попыток неудачной аутентификации, данных о сбоях и неисправностях в работе средств;

ведение электронных журналов учета технического состояния, содержащего следующие обязательные поля: информация о состоянии интерфейсов (портов), информация об ошибках работы оборудования с их классификацией, информация о загрузке и инициализации программно-аппаратных средств и их останова;

защиту электронных журналов регистрации от стирания и редактирования;

автоматическое извещение о заполнении электронного журнала регистрации с возможностью его сохранения на внешнем носителе;

ведение электронных журналов регистрации с привязкой к единому источнику времени.

19.4. При осуществлении обновления программных компонентов и служебных баз данных средства должны обеспечивать:

обновление без потери информации, необходимой для функционирования средств;

обновление только администраторами;

возврат к предыдущему состоянию в случае сбоя процесса обновления (данное положение может быть выполнено в том числе путем осуществления предварительного резервного копирования и последующего восстановления).

19.5. При осуществлении самотестирования и контроля целостности ПО средства должны обеспечивать:

контроль целостности ПО и конфигурационных файлов при загрузке, во время функционирования и по команде администратора;

возможность штатного самотестирования ПО в процессе функционирования с регистрацией указанной информации в электронном журнале регистрации.

19.6. При осуществлении резервирования и восстановления средства должны обеспечивать:

возможность создания резервной копии конфигурационных данных на внешнем носителе;

возможность создания резервной копии ПО на внешнем носителе;

возможность самовосстановления работоспособности при обнаружении критических ошибок в процессе функционирования.

IX. Требования к средствам в части реализации визуализации, построения сводных отчетов и хранения информации

20. Технические, программные, программно-аппаратные и иные средства, предназначенные для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ), предупреждения, ликвидации последствий компьютерных атак, в части реализации визуализации, построения сводных отчетов и хранения информации должны обеспечивать:

20.1. Представление сведений:

о событиях ИБ;

об обнаруженных компьютерных инцидентах;

об уязвимостях и недостатках в настройке объектов контролируемых информационных ресурсов;

об инфраструктуре контролируемых информационных ресурсов в виде схем;

в виде графиков и (или) диаграмм, содержащих функции перехода от визуализированного представления сведений о компьютерных инцидентах к соответствующей им информации;

хранящихся в базе данных;

справочной и другой необходимой информации.

20.2. Построение сводных отчетов путем реализации следующих возможностей:

построение отчетов с использованием таблиц, графиков, диаграмм и гистограмм, а также их визуализации на основе полученных данных;

выбор параметров, по которым строятся таблицы, графики, диаграммы и гистограммы в отчетах;

экспорт отчетов;

автоматическое формирование отчетов по расписанию, а также их автоматическая отправка в адреса.

20.3. Надежное и достоверное хранение загружаемой информации в течение заданного периода времени и постоянную доступность к ней, а также возможность экспорта хранящейся информации в исходном и в нормализованном виде.